PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2017
Wydawnictwo SAN | ISSN 2543-8190

Tom **XVIII** | Zeszyt 10 | Część **I** | ss. 139–152

Sylwia Bąk

Uniwersytet Jagielloński
Wydział Zarządzania i Komunikacji Społecznej
Instytut Ekonomii, Finansów i Zarządzania
sylwia.bak@student.uj.edu.pl

Bankowość elektroniczna jako nowy wymiar zarządzania ryzykiem operacyjnym w sektorze bankowym

Electronic Banking as a New Dimension of Operational Risk Management in the Banking Sector

Abstract: The purpose of this paper is an analysis of the role of electronic banking in the operational risk management of contemporary banks. The theoretical part provides information on the nature of risk in the banking, presentation of electronic banking as a new management area of banks and analyzing the legal requirements (regulatory requirements and recommendations) risk management in electronic banking. In the practical part of the article were included, in turn, the results of empirical research. The aim of the study was analysis of the operational risk management process on the example of the bank with identification of the methods and instruments used in this field, with particular emphasis on the degree of fulfillment of external regulations and recommendations. To the goal were used the following methods: literature studies, content analysis of legal regulations related to the functioning of electronic banking in Poland, the recommendations of the Financial Supervision for banks and the regulation of the Basel risk management in electronic banking, the bank case study and analysis of the content of the test bank (reports on the operations, consolidated financial statements and online information materials).

Key words: bank, banking sector, electronic banking, operational risk, risk management

Wstęp

We współczesnych warunkach ekonomicznych, charakteryzujących się wysoką dynamiką zmian, ryzyko jest nieodłącznym elementem zarządzania każdym podmiotem, niezależnie od branży, którą ten podmiot reprezentuje. W sektorze bankowym przyjmuje ono jednak szczególne formy oraz wymaga specjalnych metod i narzędzi zarządzania. Nowym wymiarem zarządzania ryzykiem bankowym jest bankowość elektroniczna, majaca kluczowe znaczenie dla osiągania przez banki zamierzonych celów finansowych oraz strategicznych. Najistotniejszym wymiarem bankowości elektronicznej jest zapewnienie bezpieczeństwa klientom korzystającym z jej usług, dostępnych zarówno za pośrednictwem bankowych stron internetowych, jak i dedykowanych aplikacji mobilnych.

Ryzyka związane z bankowością elektroniczną bezpośrednio wpływają na ogólny profil ryzyka bankowości, dlatego też tak istotne jest obecnie prowadzenie badań, poznanie i stosowanie odpowiednich technik, metod i koncepcji zarządzania w tym obszarze działalności banków.

Celem opracowania jest analiza roli bankowości elektronicznej w zarządzaniu ryzykiem operacyjnym współczesnych banków. Celem badania była z kolei analiza procesu zarządzania ryzykiem operacyjnym na przykładzie wybranego banku, ze szczególnym uwzględnieniem realizacji zadań wynikających z zewnętrznych regulacji oraz rekomendacji w zakresie bankowości elektronicznej. Dominującą metodę badawczą stanowiła analiza dokumentacji.

Istota ryzyka w działalności bankowej

Działalność bankowa nierozerwalnie związana jest z ryzykiem. Podejmując ryzyko, banki mają możliwość osiągania oraz pomnażania swoich zysków.

Banki oprócz najpowszechniejszej działalności kredytowej realizują szereg innych zadań finansowych i pozafinansowych. Ryzyko bankowe można najogólniej definiować jako możliwość powstania zysków i strat w wyniku niepewności co do przebiegu zjawisk związanych z działalnością bankową [Fedorowicz 1996, ss. 6–7].

Ryzyko bankowe ma wiele wymiarów, które można skategoryzować następująco [Komisja Nadzoru Finansowego 2011]:

- ryzyko kredytowe,
- ryzyko rynkowe,
- ryzyko płynności,
- ryzyko operacyjne,
- ryzyko modeli,
- ryzyko biznesowe,

- ryzyko kapitałowe,
- ryzyko zarządzania.

Celem każdego banku jest długoterminowe osiąganie rentowności przy jednoczesnym zachowaniu bezpieczeństwa. Ryzyko jest stymulatorem, który pozwala osiągać bankom zyski, ale może również doprowadzić do negatywnych konsekwencji, w tym nawet do bankructwa banku. Dlatego tak ważne jest uwzględnianie w procesach zarządczych banku odpowiedniego podejścia do ryzyka oraz zarządzania nim w oparciu o aktualny stan koniunktury, warunki otoczenia ekonomicznego oraz indywidualną sytuację majątkową banku. Zarządzanie ryzykiem bankowym nie powinno być kształtowane jedynie na podstawie przeszłych zdarzeń i doświadczeń organów nadzoru, lecz powinno też opierać się na aspekcie przyszłościowym. Należy analizować możliwe wersje wydarzeń, bazować na dostępnych prognozach oraz dokonywać zindywidualizowanych dla każdego banku analiz scenariuszowych [Iwanicz-Drozdowska 2012, ss. 12–15].

Pożądany poziom bezpieczeństwa, do którego dążą banki, może być osiągany dzięki: odpowiedniemu wyposażeniu w kapitały własne, wysokiemu poziomowi etycznemu i zawodowemu kadry zarządzającej i pracowników banku, analitycznemu doborowi kredytobiorców, zabezpieczeniu udzielanych kredytów, przestrzeganiu norm ostrożnościowych oraz restrykcjom systemu nadzoru bankowego [Janiak 2000, s. 26].

Ryzyko związane z bankowością elektroniczną jest głównie ryzykiem operacyjnym, wynikającym z nieodpowiedniego funkcjonowania procesów oraz systemów informatycznych, błędów ludzkich lub zdarzeń zewnętrznych o nieprzewidywalnym charakterze. Obejmuje ono również ryzyko związane z zewnętrznymi wymogami regulacyjnymi. Ryzyko operacyjne, według definicji Komisji Nadzoru Finansowego, można definiować jako możliwość wystąpienia straty wynikającej z niedostosowania lub zawodności procesów wewnętrznych, ludzi i systemów lub ze zdarzeń zewnętrznych, uwzględniając także ryzyko prawne [Komisja Nadzoru Finansowego 2010].

Znaczenie ryzyka operacyjnego w zarządzaniu instytucjami finansowymi, w tym bankami, wzrasta wraz z postępem technologicznym. Efektywne zarządzanie ryzykiem operacyjnym jest możliwe jedynie przy odpowiednio dostosowanym systemie informatycznym oraz zintegrowanej wiedzy pracowników i kadry zarządzającej [Zygier 2015, ss. 92–93]. Szczegółowo zmiany mające wpływ na wzrost znaczenia ryzyka operacyjnego w zarządzaniu bankami określił Bazylejski Komitet ds. Nadzoru Bankowego. Zalicza się do nich miedzy innymi [Basel Committee on Banking Supervision 2003]:

- pojawienie się ryzyka o charakterze systemowym, ze względu na intensywne wykorzystywanie zautomatyzowanych technologii,
- masowe procesy konsolidacyjne, fuzje i przejęcia,
- wzrost znaczenia outsourcingu,

- zwiększające się ryzyko bezpieczeństwa systemu oraz oszustw ze względu na wzrost wykorzystania e-commerce,
- różnorodność usług bankowych.

Bankowość elektroniczna jako nowy obszar zarządzania ryzykiem we współczesnych bankach

Bankowość internetowa i mobilna to obecnie dominujące elektroniczne kanały dystrybucji usług bankowych. Ich znaczenie w sektorze bankowym stale wzrasta (zob. tabela 1). Stosowanie bankowości elektronicznej jest korzystne nie tylko dla banków, ale również dla ich klientów, którzy dzięki przeniesieniu obsługi usług bankowych na platformy internetowe mogą zdalnie dokonywać operacji oraz zarządzać swoimi kontami. Bankowość elektroniczna umożliwia bowiem unikanie czasowych, przestrzennych oraz organizacyjnych ograniczeń występujących w kontaktach bank–klient [Polasik 2013].

Tabela 1. Bankowość elektroniczna w Polsce

Liczba klientów indywidualnych mających podpisaną umowę umożliwiającą korzystanie z bankowości internetowej (nie tylko ROR)		Liczba klientów indywidualnych, którzy przynajmniej raz w miesiącu logują się do ROR za pomocą bankowości internetowej.	
II kw. 2015	**II kw. 2016**	**II kw. 2015**	**II kw. 2016**
28 972 615	32 456 477	12 611 776	13 554 274

Źródło: opracowanie własne na podstawie: Raport PRNews.pl 2016.

Ze względu na dynamiczny rozwój bankowości elektronicznej w Polsce kadry zarządzające bankami stają przed wyzwaniem właściwej identyfikacji czynników ryzyka związanych z tą sferą działalności. Jest to szczególnie ważne również z uwagi na fakt, że istotną barierą w rozwoju bankowości elektronicznej jest bariera bezpieczeństwa. Aby pokonywać tę barierę, banki powinny opracowywać sprawnie działające systemy zarządzania tymi ryzykami. Zarządzanie ryzykiem bankowości elektronicznej staje się więc obecnie nieodłącznym elementem zarządzania każdym bankiem, który chce efektywnie rozwijać świadczenie swoich usług za pomocą zdalnych kanałów dystrybucji.

W zarządzaniu ryzykiem bankowości elektronicznej niezwykle istotne jest uwzględnianie zmian w otoczeniu. Rdzeń bankowości elektronicznej stanowią: systemy informatyczne, procesy bankowości elektronicznej, pracownicy banków oraz użytkownicy bankowości elektronicznej. Do otoczenia natomiast zalicza się [Dżega 2003]:

- dostawców usług teleinformatycznych,
- dostawców oprogramowania,
- nadzór bankowy,
- regulacje prawne,
- technologie,
- czynniki losowe.

W zarządzaniu ryzykiem bankowości elektronicznej na pierwszy plan wysuwa się ryzyko operacyjne. Aby zarządzać tym ryzykiem, banki stają przed koniecznością ciągłej aktualizacji wypracowanego systemu zarządzania. Takie aktualizacje są konieczne, jednak przeprowadzanie ich zbyt często lub wybiórczo może spowodować spadek wydajności pracy banku, a to z kolei może przełożyć się na zwiększone prawdopodobieństwo występowania błędów ludzkich i systemowych, a tym samym negatywnie wpłynąć na bezpieczeństwo usług bankowych świadczonych na platformie internetowej. Ryzyko operacyjne obejmuje też ryzyko prawne. Również w tej kategorii ryzyka konieczne są aktualizacje związane ze zmianami regulacyjnymi [Górka 2006, ss. 32–35].

Uwarunkowania prawne zarządzania ryzykiem w bankowości elektronicznej

Istnieje szereg uwarunkowań prawnych oraz zaleceń i rekomendacji, których stosowanie ma pozwolić współcześnie działającym bankom na efektywne zarządzanie ryzykiem operacyjnym, związanym z funkcjonowaniem bankowości elektronicznej.

Działalność banków regulowana jest między innymi poprzez ustawę Prawo Bankowe. W ustawie tej można znaleźć odniesienie do funkcjonowania bankowości elektronicznej. W art. 7 znajduje się zapis zezwalający na składanie oświadczeń woli związanych z dokonywaniem czynności bankowych w postaci elektronicznej oraz na sporządzanie na informatycznych nośnikach danych dokumentów związanych z czynnościami bankowymi, pod warunkiem, że dokumenty te będą w sposób należyty utworzone, utrwalone, przekazane, przechowywane i zabezpieczone [Ustawa Prawo Bankowe 2016].

Kolejną regulacją, w której znaleźć można wymogi dotyczące zarządzania ryzykiem w bankowości elektronicznej, była ustawa o Elektronicznych Instrumentach Płatniczych, a konkretnie jej 4 rozdział – Usługi bankowości elektronicznej [Ustawa o Elektronicznych Instrumentach Płatniczych 2002]. Ustawa ta została jednak uchylona 7 października 2013 r. i zastąpiona wymogami zawartymi zbiorczo w ustawie o Usługach Płatniczych [Ustawa o Usługach Płatniczych 2016].

Zasady funkcjonowania bankowości elektronicznej oraz jej bezpieczeństwa znaleźć można również w rozporządzeniu Rady Ministrów w sprawie sposobu tworzenia, utrwalania, przekazywania, przechowywania i zabezpieczania dokumentów związanych

z czynnościami bankowymi, sporządzanych na elektronicznych nośnikach informacji. Informacje zawarte w tym dokumencie, przydatne w realizacji procesów zarządzania ryzykiem banku zawarto w art. 7, 8, 9. Regulują one wymagania dotyczące bezpieczeństwa stosowania elektronicznych dokumentów bankowych. Artykuł 9 pkt 2 reguluje szczegółowo standardy zabezpieczania tych dokumentów. Zalicza się do nich [Rozporządzenie Rady Ministrów 2004]:

- systematyczne dokonywanie analizy zagrożeń,
- opracowywanie i stosowanie procedur zabezpieczenia dokumentów i systemów ich przetwarzania, w tym procedur dostępu,
- stosowanie środków bezpieczeństwa adekwatnych do zagrożeń,
- bieżącą kontrolę funkcjonowania wszystkich organizacyjnych i techniczno-informatycznych sposobów zabezpieczania, a także okresowe dokonywanie oceny skuteczności tych sposobów.

Regulacje dotyczące zarządzania ryzykiem operacyjnym związanym z bankowością elektroniczną można też znaleźć w szeregu rekomendacji Komisji Nadzoru Finansowego dla banków, głównie D, H oraz M. W tabeli 2 zawarto najważniejsze z nich.

Tabela 2. Rekomendacje KNF dla banków (D,H,M)

Rekomendacja	**Treść rekomendacji**
D dotyczy zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatyczne-go w bankach	1) Rada nadzorcza banku powinna nadzorować funkcjonowanie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, natomiast zarząd banku powinien zapewnić, aby powyższe obszary zarządzane były w sposób poprawny i efektywny. 2) Rozwiązania organizacyjne oraz zasoby ludzkie w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego banku powinny być adekwatne do jego profilu ryzyka i specyfiki działalności. 3) Bank powinien posiadać sformalizowane zasady dotyczące zarządzania infrastrukturą teleinformatyczną, zapewniające właściwe wsparcie działalności banku oraz bezpieczeństwo przetwarzanych danych. 4) Bank powinien posiadać sformalizowane zasady oraz mechanizmy techniczne zapewniające właściwy poziom kontroli dostępu logicznego do danych i informacji. 5) Bank świadczący usługi z wykorzystaniem elektronicznych kanałów dostępu powinien posiadać skuteczne rozwiązania techniczne i organizacyjne zapewniające weryfikację tożsamości i bezpieczeństwo danych oraz środków klientów, jak również edukować klientów w zakresie zasad bezpiecznego korzystania z tych kanałów. 6) W banku powinien funkcjonować sformalizowany, skuteczny system zarządzania bezpieczeństwem środowiska teleinformatycznego, obejmujący działania związane z identyfikacją, szacowaniem, kontrolą, przeciwdziałaniem, monitorowaniem i raportowaniem ryzyka w tym zakresie, zintegrowany z całościowym systemem zarządzania ryzykiem i bezpieczeństwem informacji w banku. 7) Bank powinien zapewnić zgodność funkcjonowania obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego z wymaganiami prawnymi, regulacjami wewnętrznymi i zewnętrznymi, zawartymi umowami i przyjętymi w banku standardami, 8) Obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego banku powinny być przedmiotem systematycznych, niezależnych audytów.
H dotyczy kontroli wewnętrznej w banku	1) W banku funkcjonuje efektywny system kontroli wewnętrznej, dostosowany do charakteru oraz profilu ryzyka i skali działalności banku. 2) Zarząd banku powinien opracować i wdrożyć spójną i kompleksową strukturę systemu kontroli wewnętrznej, w ramach której funkcjonują mechanizmy kontroli ryzyka, badanie zgodności działania banku z przepisami prawa i regulacjami wewnętrznymi oraz audyt wewnętrzny. 3) W bankach, z wyłączeniem banków spółdzielczych, funkcjonuje komitet audytu. 4) Mechanizmy identyfikacji, oceny i kontroli ryzyka powinny uwzględniać ocenę ilościową, jakościową, brać pod uwagę szacunek wpływu ryzyka na bezpieczeństwo banku i rentowność działalności, wiarygodność sprawozdawczości oraz przestrzeganie przepisów i regulacji. 5) System kontroli wewnętrznej powinien być zorientowany na rozpoznanie i ocenę ryzyka całego banku.

M dotyczy zarządzania ryzykiem operacyjnym w bankach	1) Zarząd banku odpowiada za opracowanie systemu zarządzania ryzykiem operacyjnym, jego wdrożenie, zapewnienie jego spójności ze strategią zarządzania tym ryzykiem. 2) W strukturach banku powinna istnieć wydzielona jednostka lub funkcja do spraw zarządzania ryzykiem operacyjnym. 3) Bank powinien realizować i dokumentować proces identyfikacji zagrożeń związanych z ryzykiem operacyjnym dla wszystkich istotnych obszarów działalności banku. 4) Zarządzanie ryzykiem operacyjnym powinno opierać się na rzetelnej ocenie ryzyka, przeprowadzonej na podstawie zatwierdzonych procedur. 5) Bank powinien posiadać system zarządzania ciągłością działania, w tym plany utrzymania ciągłości działania oraz plany awaryjne, uwzględniające profil ryzyka operacyjnego banku. 6) Bank powinien regularnie ogłaszać informacje na temat swojego podejścia do ryzyka operacyjnego służące ograniczeniu asymetrii informacji pomiędzy bankiem a jego otoczeniem.

Źródło: opracowanie własne na podstawie [Komisja Nadzoru Finansowego – Rekomendacje dla banków: D, H, M].

Wymogi formalne z analizowanego zakresu zawarte są też w regulacjach opracowanych przez Bazylejski Komitet ds. Nadzoru Bankowego, głównie w Zasadach Zarządzania Ryzykiem w Bankowości Elektronicznej (BE). Zasady te można podzielić na następujące kategorie [Bazylejski Komitet ds. Nadzoru Bankowego 2001]:

kontrola ze strony Rady i Zarządu

- efektywna kontrola bankowości elektronicznej przez kierownictwo,
- ustanowienie wszechstronnego procesu kontroli bezpieczeństwa,
- ustanowienie wszechstronnego i ciągłego procesu badania należytej staranności i kontroli zarządzania zlecaniem usług na zewnątrz oraz innych zależności od stron trzecich.

mechanizmy kontroli bezpieczeństwa

- sprawdzanie tożsamości klientów BE,
- uniemożliwienie negowania dokonanych transakcji oraz odpowiedzialność za transakcje BE,
- odpowiednie środki zapewniające podział obowiązków,
- właściwe mechanizmy kontroli upoważnień w ramach systemów, baz danych i aplikacji BE,
- rzetelność danych dotyczących transakcji, zapisów i informacji z zakresu BE,
- ustanowienie jasno określonych ścieżek audytu dla transakcji BE,
- poufność podstawowych informacji bankowych.

zarządzanie ryzykiem prawnym i reputacji

- odpowiednia sprawozdawczość dotycząca usług BE,
- poufność danych o klientach,

- pojemność systemu, zapewnienie ciągłości działalności i planowanie awaryjne w celu zapewnienia dostępności systemów i usług BE,
- plany reagowania na incydenty.

Na podstawie szczegółowej analizy wszystkich rekomendacji wchodzących w skład Zasad Zarządzania Ryzykiem w BE można przedstawić sześć kluczowych wymiarów, których sprawne funkcjonowanie pozwoli właściwie zarządzać tą sferą działalności banków:

- kontrola bezpieczeństwa w BE,
- autoryzacja dostępu do aplikacji BE,
- ścieżki audytu w systemach BE,
- zachowanie poufności informacji o klientach BE,
- zdolność świadczenia usług, ciągłość działania i planów awaryjnych dotyczących BE.

Zarządzanie ryzykiem operacyjnym w wybranym banku wraz z oceną spełnienia wymogów regulacyjnych i zaleceń rekomendacji z zakresu bankowości elektronicznej

Metodyka badań empirycznych

Głównym celem badawczym jest analiza procesu zarządzania ryzykiem operacyjnym na przykładzie wybranego banku, ze szczególnym uwzględnieniem realizacji zadań wynikających z zewnętrznych regulacji oraz zaleceń dotyczących bankowości elektronicznej. Jako przedmiot badawczy w tej części wybrano mBank. W procesie badawczym zostały wykorzystane następujące metody: analiza treści dokumentacji badanego banku (sprawozdań zarządów z działalności, skonsolidowanych sprawozdań finansowych oraz innych internetowych materiałów informacyjnych – w tym raportów rocznych online) oraz studium przypadku wybranego banku.

mBank wybrany jako przedmiot badawczy w niniejszym opracowaniu jest jednym z liderów bankowości elektronicznej w Polsce. Na koniec 2014 r. posiadał największą liczbę użytkowników bankowości mobilnej w skali kraju (892 tys.). Ponadto rokrocznie znajduje się na czołowych miejscach w rankingu „Przyjazny Bank Newsweeka" w kategoriach: bankowość mobilna (zwycięstwo w roku 2016) i bankowość internetowa.

mBank efektywnie realizuje proces zarządzania ryzykiem operacyjnym, uwzględniający realia funkcjonowania bankowości elektronicznej. Grupa mBanku zarządza ryzykiem w oparciu o wymagania nadzorcze oraz najlepsze praktyki rynkowe, formułując strategie, polityki oraz wytyczne w zakresie zarządzania ryzykiem. Posiada wdrożoną i aktualizowaną Strategię Zarządzania Ryzykiem oraz strategie zarządzania poszczególnymi kategoriami ryzyka (w tym Strategię Zarządzania Ryzykiem Operacyjnym).

Ryzyko związane z bankowością elektroniczną mBank lokuje w kategorii ryzyka operacyjnego. Przez ryzyko operacyjne mBank rozumie możliwość poniesienia straty wynikającej z nieadekwatnych lub wadliwych wewnętrznych procesów, systemów, błędów lub działań podjętych przez pracownika banku oraz ze zdarzeń zewnętrznych. Organizując proces zarządzania ryzykiem operacyjnym, mBank kieruje się zasadami i wymaganiami zawartymi w Uchwale KNF Nr 76/2010 z dnia 10 marca 2010 r. oraz Rozporządzeniu Parlamentu Europejskiego i Rady UE nr 575/2013 z dnia 26 czerwca 2013 r. Wspomniane uchwały, a także rekomendacje Komisji Nadzoru Finansowego (w tym zwłaszcza Rekomendacja M, H oraz D) stanowią punkt wyjścia dla przygotowania ram systemu kontroli i zarządzania ryzykiem operacyjnym w Grupie mBanku. Zgodnie z Katalogiem Ryzyka Grupy mBanku S.A. ryzyko operacyjne obejmuje w szczególności następujące podkategorie:

- ryzyko prawne,
- ryzyko działania systemów informatycznych,
- ryzyko kadrowe i organizacyjne,
- ryzyko bezpieczeństwa,
- ryzyko braku zgodności.

Na kontrolę i zarządzanie ryzykiem operacyjnym składa się zbiór działań mających na celu identyfikację, monitorowanie, pomiar, ocenę, raportowanie, a także redukcję, unikanie, transfer lub akceptację ryzyka operacyjnego, na które mBank jest narażony w poszczególnych obszarach działalności. Podstawą kontroli ryzyka operacyjnego są metody oraz narzędzia ilościowe i jakościowe. Podstawowym narzędziem jakościowym jest samoocena systemu kontroli wewnętrznej wykonywana przez jednostki organizacyjne mBanku.

mBank spełnia również wymogi regulacyjne wszystkich kategorii zawartych w Zasadach Zarządzania Ryzykiem w BE stworzonych przez Bazylejski Komitet ds. Nadzoru Bankowego. W poszczególnych wymiarach kolejno realizuje zadania, takie jak:

a) kontrola bezpieczeństwa

- kontrola bezpieczeństwa i ryzyka, w tym także związanego z BE, sprawowana jest przez: Radę Nadzorczą, Zarząd, Komisję ds. Ryzyka, Wiceprezesa Zarządu ds. Zarządzania Ryzykiem, Departament Bezpieczeństwa, Komitet Ryzyka, Komitet Forum Biznesu i Ryzyka;
- za proces monitorowania i kontroli ryzyka operacyjnego odpowiada Departament Zarządzania Zintegrowanym Ryzykiem i Kapitałem;
- za zarządzanie aplikacjami IT Ryzyka (biznesowe utrzymanie i rozwój) odpowiada Departament Zarządzania Projektami i Architekturą Ryzyka.

b) autoryzacja dostępu do aplikacji bankowości elektronicznej

- bezpieczne logowanie, autoryzacja transakcji, szyfrowane połączenie z systemem;
- proces „parowania" urządzenia i unikalny PIN;
- informowanie klientów o zasadach bezpieczeństwa korzystania z BE i autoryzacji dostępu poprzez publikację „Dekalogu bezpieczeństwa w Internecie" oraz zakładkę na stronie internetowej „Bezpieczeństwo w mBanku" (m.in. Złote zasady bezpieczeństwa, Bezpieczny bank w komputerze, Bezpieczny bank w telefonie i tablecie).

c) ścieżki audytu w systemach bankowości elektronicznej

- w Grupie mBanku role i zadania w zakresie zarządzania ryzykiem zorganizowano w oparciu o model trzech linii obrony:
  - pierwszą linię obrony stanowi Biznes (linie biznesowe), odpowiedzialny za zarządzanie ryzykiem i kapitałem,
  - druga linia obrony, przede wszystkim Ryzyko (obszar zarządzania ryzykiem), Bezpieczeństwo IT oraz funkcja Compliance wspiera Biznes, tworząc strategie zarządzania poszczególnymi rodzajami ryzyka oraz odpowiednie polityki określające wytyczne dla Biznesu odnoszące się do decyzji związanych z podejmowaniem ryzyka przez Biznes,
  - trzecią linią obrony jest Audyt Wewnętrzny, dokonujący niezależnych ocen zarówno pierwszej, jak i drugiej linii obrony;
- działanie systemu kontroli wewnętrznej obejmującego: kontrolę funkcjonalną, monitorowanie i mechanizmy kontroli ryzyka, badanie zgodności działania banku z przepisami prawa i regulacjami wewnętrznymi oraz audyt wewnętrzny.
- za realizację procesu audytu wewnętrznego odpowiedzialny jest Departament Audytu Wewnętrznego,
- istnieje Komisja ds. Audytu;

d) zachowanie poufności informacji o klientach

- zapewnienie klientom poufności danych osobowych,
- istnienie Komitetu Ochrony Danych,
- zapewnienie pełnego bezpieczeństwa wymienianych z bankiem informacji,
- polityka prywatności mBanku oraz polityka prywatności aplikacji mobilnych zgodne z wymogami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz Ustawy z dnia 29 sierpnia 1997 roku Prawo bankowe;

f) zdolność świadczenia usług, ciągłości działania i planów awaryjnych dotyczących bankowości elektronicznej

- w celu kontroli ryzyka operacyjnego i zapewnienia ciągłości działania mBank prowadzi rejestr zdarzeń i strat operacyjnych Grupy, zbiera i monitoruje kluczowe wskaźniki ryzyka, a także tworzy i analizuje scenariusze ryzyka operacyjnego w celu identyfikacji zdarzeń, które potencjalnie mogą spowodować bardzo duże straty o charakterze operacyjnym, również z zakresu bankowości elektronicznej,

- utrzymywana jest komunikacja z wszystkimi obszarami działania Banku w celu monitorowania i podjęcia działań zapobiegawczych w momencie zasygnalizowania ryzyka krytycznych zdarzeń w jakimkolwiek obszarze działania,
- zapewnianie zdolności świadczenia usług i ciągłego rozwoju w zakresie BE, m.in. poprzez funkcjonowanie Komitetu ds. Jakości Danych i Rozwoju Systemów Informacyjnych;
- stałe tworzenie planów awaryjnych (głównie metodą analizy scenariuszowej) oraz awaryjnego planu ciągłości działania, który obejmuje systemy informatyczne odpowiedzialne za sprawne funkcjonowanie BE;
- funkcjonowanie Komitetu ds. Architektury Informatycznej.

Zakończenie

Ciągłe innowacje technologiczne oraz wzrost konkurencyjności pomiędzy instytucjami bankowymi umożliwiają klientom dostęp do szerokiego zakresu usług i produktów bankowych oraz dostarczanie ich dzięki wykorzystaniu bankowości elektronicznej, czyli elektronicznych kanałów dystrybucji. Dynamiczny rozwój bankowości elektronicznej niesie jednak za sobą oprócz szeregu korzyści liczne ryzyka. Dlatego istotnym obszarem działalności współczesnych banków jest identyfikacja tych ryzyk i zarządzanie nimi w sposób ostrożnościowy, zgodnie ze specyfiką bankowości elektronicznej, wymogami regulacyjnymi oraz zaleceniami instytucji nadrzędnych. Ważne jest, że uwarunkowania prawne dla zarządzania ryzykiem w bankowości tradycyjnej są nadal aktualne dla bankowości elektronicznej, jednak wymagają odpowiedniego dostosowania do nowych systemów i procesów realizowanych w tym obszarze działalności bankowej, głównie w kategorii ryzyka operacyjnego, które w największym stopniu zostało zwiększone i zmodyfikowane w związku z rozwojem bankowości elektronicznej [Komisja Nadzoru Finansowego 2001]. Istnieją też odrębne dokumenty i rekomendacje zawierające zbiory reguł już dostosowanych do realiów zarządzania ryzykiem w elektronicznej sferze działalności banków.

Przeprowadzona analiza procesu zarządzania ryzykiem operacyjnym mBanku dowiodła, że spełnia on wymogi regulacyjne oraz zalecenia rekomendacji dotyczące bankowości elektronicznej.

Bibliografia

Dżega D. (2003), *(Nie)bezpieczny e-bank*, „Internet", nr 10.

Fedorowicz Z. (1996), *Ryzyko bankowe,* Wydawnictwo Prywatnej Wyższej Szkoły Businessu i Administracji, Warszawa.

Górka J. (2006), *Specyfika ryzyka bankowości elektronicznej*, „Materiały i Studia", nr 205, Narodowy Bank Polski.

Iwanicz-Drozdowska M. (red.) (2012), *Zarządzanie ryzykiem bankowym*, POLTEXT, Warszawa.

Janiak A. (2000), *O przywilejach bankowych*, cz. II, „Prawo Bankowe", nr 10.

Komisja Nadzoru Finansowego (2010), Załącznik nr 14 do Uchwały nr 76/2010 (Dz. Urz. KNF Nr 2, poz. 11 z późn. zm.).

Polasik M. (2013), *Wykorzystanie elektronicznych kanałów dystrybucji usług bankowych w Polsce,* „Copernican Journal of Finance & Accounting", Vol. 2, Iss. 1.

Rozporządzenie Rady Ministrów z dnia 26 października 2004 r. w sprawie sposobu tworzenia, utrwalania, przekazywania, przechowywania i zabezpieczania dokumentów związanych z czynnościami bankowymi, sporządzanych na elektronicznych nośnikach informacji (Dz.U. z 2004 r. Nr 236 poz. 2364).

Ustawa o Elektronicznych Instrumentach Płatniczych z dnia 12 września 2002 r. (Dz.U. 2002 nr 169 poz. 1385).

Ustawa o usługach płatniczych (Dz.U. z 2016 r., poz. 1572).

Ustawa Prawo bankowe (Dz. U. z 2016 r., poz. 1988).

Zygier M. (2015), *Charakterystyka i znaczenie ryzyka operacyjnego w działalności bankowej,* „Nauki o Zarządzaniu", nr 1(22).

Bibliografia elektroniczna

Basel Committee on Banking Supervision (2003*), Sound Practices for the Management and Supervision of Operational Risk,* [online] http://www.bis.org/publ/bcbs96.pdf, dostęp: 15.01.2017.

Bazylejski Komitet ds. Nadzoru Bankowego (2001), *Zasady zarządzania ryzykiem w bankowości elektronicznej*, [online] https://www.knf.gov.pl/Images/electronic_tcm75-4713.pdf, dostęp: 16 stycznia 2017.

Komisja Nadzoru Finansowego (2011), *BION w bankach – mapa klas ryzyka i ich definicje*, [online] https://www.knf.gov.pl/Images/banki_mapa_ryzyk_tcm75-25314.pdf, dostęp: 13.01.2017.

Komisja Nadzoru Finansowego – Rekomendacje dla banków: D,H,M, [online] https://www.knf.gov.pl/regulacje/praktyka/rekomendacje_banki/rekomendacje.html, dostęp: 17.01.2017.

mBank – Raport roczny 2015, [online] https://www.mbank.pl/raport-roczny/2015/, dostęp: 18.01.2017.

mBank – Raport roczny 2014, [online] http://raportroczny.mbank.pl/raport/spis-tresci/, dostęp: 18.01.2017.

mBank – Nota objaśniająca zarządzania ryzykiem, [online] https://www.mbank.pl/pdf/raport-roczny/noty-objasniajace/zarzdzanie-ryzykiem.pdf, dostep: 18.01.2017.

Raport PRNews.pl, *Rynek bankowości internetowej – II kw. 2016,* [online] http://prnews.pl/raporty/raport-prnewspl-rynek-bankowosci-internetowej-ii-kw-2016-6553183.html, dostep: 16 stycznia 2017.

Skonsolidowane Sprawozdanie Finansowe Grupy mBanku za 2015 rok, [online] https://www.mbank.pl/pdf/raport-roczny/mbank-raport-roczny-2015-pl_ver1.pdf, dostęp: 18.01.2017.

Sprawozdanie Zarządu z działalności Grupy mBanku S.A. w 2015 roku, [online] https://www.mbank.pl/pdf/raport-roczny/mbank-raport-roczny-2015-pl_ver1.pdf, dostęp: 18.01.2017.